Abstract

A system for real-time vulnerability assessment of a host/device, said system comprising an agent running on the host/device. The agent includes a a first data structure for storing the status of interfaces and ports on the interfaces of the host/device. An n executable agent module is coupled to the first data structure to track the status of interfaces and ports on the interfaces of the host/device and to store the information, as entries in said first data structure. The executable agent module compares the entries to determine a change in the status of interfaces and/or of ports on the interfaces of the host/device. A remote destination server is provided that includes a second data structure for storing the status of interfaces and the ports on the interfaces of the host/device. An executable server module is coupled to the second data structure to receive the information communicated by the agent executable module of the agent on the host/device. The executable server module stores the received information as entries in the second data structure wherein the entries indicate the state of each of the ports on each of the active interfaces of the host/device as received. The executable server module compares the entries in said data structures to determine the change in the status of interfaces and ports on the interfaces of the host/device. The executable server module runs vulnerability assessment tests on the host/device in the event of a change in the status of interface/ports.